【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年7月8日(2004.7.8)

【公開番号】特開2003-204320(P2003-204320A)
【公開日】平成15年7月18日(2003.7.18)
【出願番号】特願2002-303509(P2002-303509)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/08
【ＦＩ】
　Ｈ０４Ｌ　9/00　６０１Ｂ
　Ｈ０４Ｌ　9/00　６０１Ａ

【手続補正書】
【提出日】平成15年6月2日(2003.6.2)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置と、１以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、
前記鍵管理装置は、
ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と

を備えることを特徴とする著作物保護システム。
【請求項２】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、
ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項３】
前記ｎ分木は、複数のレイヤから構成され、
前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、
前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項４】
前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、
前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項５】
前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成する
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項６】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成する
ことを特徴とする請求項２に記載の鍵管理装置。
【請求項７】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報と

から構成される特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報を生成する
ことを特徴とする請求項６に記載の鍵管理装置。
【請求項８】
前記無効化情報生成手段は、
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報を生成し、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報を生成する
ことを特徴とする請求項６に記載の鍵管理装置。
【請求項９】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、
ｎ分木において一部のノードは、無効化されており、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、
リーフを除き、無効化された各ノードについて、
下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、
下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、
その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、
得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項１０】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、ｎ分木を構成する全てのノードは、有効であり、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、
各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込む鍵情報生成手段と、
ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込む無効化情報生成手段と
を備えることを特徴とする鍵管理装置。
【請求項１１】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個

のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項１２】
前記ｎ分木は、複数のレイヤから構成され、
前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１３】
前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、
前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１４】
リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、
前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１５】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１１に記載の利用者装置。
【請求項１６】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第１付加情報と、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第２付加情報と、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１５に記載の利用者装置。
【請求項１７】
リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位のｎ個のノードのそれぞれが無効化されていることを示すｎ桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、
前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、
リーフを除く他の無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示すｎ桁の無効化情報が生成されて前記記録媒体に書き込まれ、
前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する
ことを特徴とする請求項１５に記載の利用者装置。
【請求項１８】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位のｎ個のノードの少なくとも１個が無効化されている場合に、それぞれが無効化されているか否かを示す第１無効化情報を生成し、下位のｎ個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第２無効化情報を生成し、その結果、１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報が得られ、得られた１個以上の第１無効化情報、１個以上の第２無効化情報、又は１個以上の第１無効化情報及び１個以上の第２無効化情報を

、前記配列順序に従って前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に前記配列順序に従って書き込まれた前記第１無効化情報、前記第２無効化情報、又は前記第１無効化情報及び前記第２無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項１９】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ｎ分木を構成する全てのノードは、有効であり、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込み、ｎ分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込み、
前記利用者装置は、
前記記録媒体に有効であることを示す前記情報が記録されていると判断する場合に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出す読出手段と、
読み出した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と
を備えることを特徴とする利用者装置。
【請求項２０】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムであって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理プログラムは、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと
を含むことを特徴とする鍵管理プログラム。
【請求項２１】

ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムであって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用者プログラムは、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと
を含むことを特徴とする利用者プログラム。
【請求項２２】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理方法であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理方法は、
無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵をそれぞれ用いて、１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと
を含むことを特徴とする鍵管理方法。
【請求項２３】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用方法であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノード

は、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用方法は、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと
を含むことを特徴とする利用方法。
【請求項２４】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記鍵管理装置は、ｎ分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しているデバイス鍵記憶手段を備え、
前記鍵管理プログラムは、
複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、
リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと
を含むことを特徴とする記録媒体。
【請求項２５】
ｎ分木（ｎは、２以上の整数）に関連付けて１個以上のデバイス鍵を有する鍵管理装置により、１以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き

、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、
前記利用者プログラムは、
前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、
特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、
生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと
を含むことを特徴とする記録媒体。
【請求項２６】
コンピュータ読み取り可能な記録媒体であって、
ｎ分木（ｎは、２以上の整数）の構成に係る配列順序に従って、複数の暗号化メディア鍵及び複数の無効化情報を記録しており、
ここで、前記複数の暗号化メディア鍵及び前記複数の無効化情報は、鍵管理装置により生成され、記録され、前記鍵管理装置は、ｎ分木に関連付けて１個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当て、
前記鍵管理装置は、ｎ分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて１個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、１以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、ｎ分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のｎ個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む
ことを特徴とする記録媒体。
【請求項２７】
対象物の無効化を管理する無効化管理装置と対象物が無効か否かを判定する無効判定装置とから構成される認証システムであって、
前記無効化管理装置は、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、前記木構造を構成する複数のノードを有する木構造記憶手段と、
リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成する無効化リスト生成手段と、
生成した無効化リストを出力する出力手段とを含み、
前記無効判定装置は、
前記木構造の１個のリーフを示すリーフ識別子であり、対象物を識別する識別子を取得する識別子取得手段と、
前記無効化リストを取得するリスト取得手段と、

取得した前記無効化リスト内に配列されている前記無効化情報を用いて、ルートから前記リーフに至る経路の構築を試み、構築された経路内に前記リーフが含まれる場合に、前記対象物が無効であると判断し、前記リーフが含まれない場合に、前記対象物が有効であると判断する判定手段と、
前記対象物が無効であると判断される場合に、前記対象物の利用を禁止し、前記対象物が有効であると判断される場合に、前記対象物を利用する利用手段とを含む
ことを特徴とする認証システム。
【請求項２８】
対象物の無効化を管理する無効化管理装置であって、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、前記木構造を構成する複数のノードを有する木構造記憶手段と、
リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成する無効化リスト生成手段と、
生成した無効化リストを出力する出力手段と
を備えることを特徴とする無効化管理装置。
【請求項２９】
対象物が無効か否かを判定する無効判定装置であって、
無効化管理装置は、木構造を構成する複数のノードを有し、前記木構造の複数のリーフは、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうち少なくとも１個の対象物が無効化されており、無効化された対象物を識別するリーフ識別子により示されるリーフからルートに至るまでの全てのノードは無効化されており、リーフを除く無効化された各ノードについて、下位のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記木構造の構成に係る配列順序に従って配列して無効化リストを生成し、生成した無効化リストを出力し、
前記無効判定装置は、
前記木構造の１個のリーフを示すリーフ識別子であり、対象物を識別する識別子を取得する識別子取得手段と、
前記無効化管理装置から前記無効化リストを取得するリスト取得手段と、
取得した前記無効化リスト内に配列されている前記無効化情報を用いて、ルートから前記リーフに至る経路の構築を試み、構築された経路内に前記リーフが含まれる場合に、前記対象物が無効であると判断し、前記リーフが含まれない場合に、前記対象物が有効であると判断する判定手段と、
前記対象物が無効であると判断される場合に、前記対象物の利用を禁止し、前記対象物が有効であると判断される場合に、前記対象物を利用する利用手段と
を備えることを特徴とする無効判定装置。
【請求項３０】
対象物の無効化に係る無効化リストを記録しているコンピュータ読取り可能な記録媒体であって、
無効化管理装置は、
木構造の複数のリーフが、それぞれ複数の対象物に対応し、各リーフを示すリーフ識別子は、各対象物を識別し、前記対象物のうちいずれも無効化されておらず、全てのノードは、無効化されておらず、前記木構造を構成する複数のノードを有する木構造記憶手段と、
木構造を構成する全てのノードは、無効化されていないと判断し、無効化された対象物が存在しないことを示す無効化リストを生成する無効化リスト生成手段とを含み、

前記記録媒体は、生成された前記無効化リストを記録している
ことを特徴とする記録媒体。